Date of Hearing: April 20, 2016

ASSEMBLY COMMITTEE ON GOVERNMENTAL ORGANIZATION
Adam Gray, Chair
AB 2595 (Linder) – As Amended March 30, 2016

SUBJECT: California Cybersecurity Integration Center

SUMMARY: Establishes the California Cybersecurity Integration Center, tasked with reducing the likelihood and severity of a cyberattack in California, developing a cybersecurity strategy for California, and authorizes the administration of federal homeland security grant funding by the Office of Emergency Services. Specifically, **this bill**:

1) Establishes the California Cybersecurity Integration Center (Cal-CSIC) within the Governor's Office of Emergency Services (CalOES).

2) Requires Cal-CISC to develop a cybersecurity strategy for California in coordination with the Cybersecurity Task Force (Task Force), and in accordance with state and federal requirements, consistent with applicable standards and best practices.

3) Declares the primary mission of Cal-CISC to be the reduction of the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or public and private sector computer networks in our state.

4) Requires the Cal-CISC to include, but not be limited to, representatives of CalOES, the California Department of Technology's Office of Information Security (OIS), the State Threat Assessment Center, the California Highway Patrol, the California Military Department, the Office of the Attorney General, the California Health and Human Services Agency, the California Utilities Emergency Association, the California State University, the University of California and the California Community Colleges.

5) Authorizes the Director of CalOES, in consultation with OIS or the Task Force, to administer, authorize, and allocate federal homeland security grant funding in accordance with federal grant guidelines, and shall prioritize grant funding for prevention measures undertaken by the OIS in furtherance of the provision in the Governor's Executive order B-34-15 that directs state departments and agencies to "ensure compliance with existing information security and privacy policies, promote awareness of information security standards with their workforce."

6) Provides that this authorization shall not preclude the Director of CalOES from administering the grant programs to respond to statewide emergencies requiring immediate attention.

7) Defines the terms "prevention measures" and "Federal homeland security grant funding."

EXISTING LAW:

1) Establishes CalOES by the Governor's Reorganization Plan No.2, operative July 1, 2013.

2) Requires CalOES to perform a variety of duties with respect to specified emergency preparedness, mitigation, and response activities in the state, including emergency medical services.
3) Requires the Governor and CalOES, pursuant to the California Emergency Services Act (CESA), to prepare for and mitigate the effects of emergencies in the state.

4) Requires CalOES, and its appointed Director, to perform a variety of duties with respect to specified emergency preparedness, mitigation, and response activities in the state, including emergency medical services.

5) Establishes, within the California Department of Technology (CDT), the Office of Information Security to ensure the confidentiality, integrity, and availability of state systems and applications, and to promote and protect privacy as part of the development and operations of state systems and applications to ensure the trust of the residents of this state.

FISCAL EFFECT: Unknown

COMMENTS:

Purpose of this bill: According to the author, "In 2013, Governor Brown reorganized government to address the growing needs of technology by creating the California Department of Technology and the Cybersecurity Task Force, which is co-chaired by the department and the Governor's Office of Emergency Services. Since that time, however, there has been no accounting of federal homeland security grant dollars that could be used to fund cybersecurity prevention efforts by the state. There has been no scrutiny by the State Auditor or the Legislature in an oversight role to determine whether those funds are being spent wisely or for the right purposes."

"AB 2595 is needed to require the Office of Emergency Services to administer homeland security grant funding in a way that would be beneficial for the state to reach its proper prevention levels to protect against a cyberattack, intrusion, or data breach."

Background: In 2009, the California Legislature merged the powers, purposes, and responsibilities of the former CalOES with those of the Office of Homeland Security (OHS) into the newly- created California Emergency Management Agency (CalEMA).On July 1, 2013, Governor Edmund G. Brown Jr.'s Reorganization Plan #2 eliminated CalEMA and restored it to the Governor's Office, renaming it the California Governor's Office of Emergency Services (CalOES), and merging it with the Office of Public Safety Communications. Today, CalOES is responsible for overseeing and coordinating emergency preparedness, response, recovery and homeland security activities within the state.

Additionally, CESA authorizes the Governor to take actions to prepare for, respond to, and prevent natural or human-caused emergencies that endanger life, property, and the state's resources, and further authorizes CalOES and its Director to take actions to coordinate emergency planning, preparedness, and response activities. On August 31, 2015, Governor Brown, under the authority of CESA, signed Executive Order B-34-15.

Executive Order B-34-15 (EO): Governor Brown signed Executive Order B-34-15 (EO) which noted the increasing number and complexity of cyberattacks against public and private networks, and in response announced the establishment of the California Cybersecurity Integration Center

(Cal-CISC).

Cal-CISC is charged with reducing the likelihood and severity of a damaging cyber incident in California, and would serve as the "central organizing hub" of state government's cybersecurity activities and coordinate information sharing" with a variety of government agencies. It would be comprised of representatives from 15 different state and federal public entities.

Its main purposes would be threat information sharing, risk assessment, threat prioritization, supporting governmental audits and accountability measures, enabling cross-sector coordination and sharing of best practices. Cal-CISC would be responsible for developing a statewide cybersecurity strategy. It would also be charged with establishing a Cyber Incident Response Team (CIRT) to serve as California's primary unit to lead cyber threat detection, reporting, and response in coordination with public and private entities across the state. CIRT would also provide assistance to law enforcement agencies with primary jurisdiction over cyber-crimes and state government cybersecurity. The team would be populated with staff from the agencies, departments and organizations represented on Cal-CISC.

The authorization provided by this bill differs from the EO in a few substantial ways. This bill omits four federal partner agencies and other members designated by CalOES, although it does not strictly exclude them. Also, the bill omits any mention of the creation of a Cyber Incident Response Team, and also does not require that information sharing be conducted in a manner that protects the privacy and civil liberties of individuals, safeguards sensitive information, and preserves business confidentiality. It should be noted that the Executive Branch already has the authority to create and operate Cal-CISC, which is now far along in the development stage. Codification would simply remove the Governor's authority to unilaterally change any of the provisions added to statute.

Homeland security grant funding: According to the author, "OES is responsible for $1.6 billion in federal grant funding". Of that total, there are two federal grants intended to fund prevention programs: the State Homeland Security Program, which "provides grant funds to address prevention in urban areas", and the Urban Areas Security Initiative, which "funds address the unique risk-driven and capabilities–based planning, organization, equipment, training, and exercise needs of high density urban areas." The author contends that these two programs total $180 million in federal funding for homeland security efforts in California, but "there has been no accounting of these federal homeland security grant dollars that could be used to fund cybersecurity prevention efforts for Californians."

As noted by the Committee on Privacy and Consumer Protection, the practical effect of the language of this bill is to authorize the Director of CalOES to administer, authorize and allocate federal homeland security grant funding, and to prioritize that grant funding (except in state emergencies) for preventative measures taken by OIS to ensure compliance by state departments and agencies with existing information security standards and policies, including the performance of risk assessments. There is no clear reason to believe that the Director of CalOES lacks the authority to administer and allocate such federal grants, as such administration has been ongoing for years.

Policy Considerations:

1. Should AB 2595 become law, it would place only a portion of the EO in statute. As stated above, the Governor, under the authority of CESA, signed B-34-15. The contents in the EO do not need to be codified in statute for the directions/orders of the Governor to be realized. However, it certainly does not hurt and could provide for additional accountability for all involved agencies and remove the Governor's authority to unilaterally change any of the provisions added to statute. *The Committee may wish to consider whether it is necessary to codify the EO in statute. If yes, the Committee and author may wish to consider adding the entire EO into statute.*

2. Should AB 2595 become law, it would bill authorize the Director of CalOES to administer, authorize and allocate federal homeland security grant funding. As stated above, there is no clear reason to believe that the Director lacks the authority to administer and allocate said federal grant funds. *Should the intent of AB 2595 be to provide more transparency or allocation control of federal homeland security grants funds, the Committee and author may wish to consider whether or not more specific provisions related to transparency or allocation control is appropriate, such as a requirement to annually report online any expenditures or allocations of federal homeland security grants funds.*

Related legislation. AB 1841 (Irwin) of 2015/2016 Session. Would requires CalOES to develop, by July 1, 2017, a statewide emergency services response plan for cybersecurity attacks against critical infrastructure, and further requires OES to develop a comprehensive cybersecurity strategy by July 1, 2018, with which all state agencies must report compliance by January 1, 2019. AB 1841 is currently pending in the Assembly Governmental Organization Committee.

AB 1881 (Chang) of 2015/2016 Session. Would requires the Director of the California Department of Technology to develop and update mandatory baseline security controls for state networks based on industry and national standards, and annually measure the state's progress towards compliance. AB 1881 is currently pending in the Assembly Privacy and Consumer Protection Committee.

SB 949 (Jackson) of 2015/2016 Session. Would authorize the Governor to require owners and operators of critical infrastructure to submit critical infrastructure information to OES or any other designee for the purposes of gathering, analyzing, communicating, or disclosing critical infrastructure information. SB 949 is pending hearing in the Senate Governmental Organizations Committee.

Double-referral. This bill has been double referred to Assembly Committee on Privacy and Consumer Protection and is scheduled to be heard in on Tuesday, April 19.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

None on file

Analysis Prepared by: Kenton Stanhope / G.O. / (916) 319-2531